United States Naval War College
Newport, Rhode Island

THE INFORMATION WARFARE THREAT TO AIR EXPEDITIONARY FORCES

by

Richard E. Pearcy

Major, USAF

A paper submitted to the faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Richard E. Pearcy
Signature

8 February 2000

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED

2. Security Classification Authority:

3. Declassification/Downgrading Schedule:

4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

5. Name of Performing Organization:
JOINT MILITARY OPERATIONS DEPARTMENT

6. Office Symbol: C	**7. Address:** NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207

8. Title (Include Security Classification):
The Information Warfare Threat to Air Expeditionary Forces (UNCLASSIFIED)

9. Personal Authors:
Richard E. Pearcy, Major, USAF

10.Type of Report: FINAL	**11. Date of Report:** 8 February 2000
12.Page Count: 20 [redacted]	**12A Paper Advisor (if any):**

13.Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. Ten key words that relate to your paper: military, information, expeditionary, warfare, air force, threat, vulnerability, technology, denial, interference

15.Abstract: In October 1999, the United States Air Force successfully deployed the first full-scale Air Expeditionary Force, marking the final step in the transition from a Cold War era, forward-based presence force to one built and shaped for quick and decisive global engagement. Each Air Expeditionary Force (AEF) consists of a small cross-section of aerospace forces, tailored by task, prepared to rapidly deploy and operate from well-established bases or geographically isolated, bare base airfields with minimal infrastructure. The AEF depends on external support for sustained operations, especially during deployment to remote locations. Advanced information and communication systems provide the critical link between the AEF and the Air Force's worldwide support network. This heavy reliance on information connectivity increases the AEF's vulnerability to information warfare (IW) attack. The IW threat to the AEF is significant. Potential adversaries continue to develop the technology and doctrine necessary to employ increasingly effective IW against the United States and its allies, ensuring the role of IW as a powerful weapon now and in future conflicts. This paper examines the major information systems used by a remotely deployed AEF, identifies the vulnerabilities of those systems to IW attack, assesses the impact of hostile IW on operations, and highlights important factors for the AEF commander to consider when developing a strategy to deter, detect, negate, and recover from IW attack.

16.Distribution / Availability of Abstract:	**Unclassified** X	**Same As Rpt**	**DTIC Users**

17.Abstract Security Classification: UNCLASSIFIED

18.Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT

19.Telephone: 841-6461	**20.Office Symbol:** C

Security Classification of This Page Unclassified

ABSTRACT

In October 1999, the United States Air Force (USAF) successfully deployed the first full-scale Air Expeditionary Force (AEF) to support contingency operations in Southwest Asia. This AEF deployment was the final step in the USAF's transition from a Cold War era, forward-based presence force to one built and shaped for global engagement. Each AEF consists of a cross-section of aerospace forces, tailored to handle a broad range of missions. These deployable forces can operate from well-established bases or geographically isolated, bare base airfields with minimal infrastructure. The AEF maintains a light but powerful logistical and force footprint by leveraging communications and information technology to sustain long-term operations as well as bolster combat effectiveness. This heavy reliance on communication and information systems, particularly during deployment to isolated areas with minimal or no supporting infrastructure, increases the vulnerability and susceptibility to information warfare (IW) attack. Potential adversaries continue to develop the technology and doctrine necessary to employ IW in asymmetric warfare against the United States and its allies, ensuring the role of IW as a dominant force in future conflicts. This paper examines the major communications and information systems used by a typical AEF, identifies potential IW vulnerabilities, and recommends specific steps to reduce the susceptibility to IW attack. The IW threat to expeditionary aerospace forces is very real and dangerous. Studying and understanding the nature of the threat will allow commanders at all levels to accurately assess the risk and better coordinate actions to deter, detect, negate, and recover from IW attacks.

INTRODUCTION

In October 1999, the United States Air Force successfully deployed the first full-scale Air Expeditionary Force to support contingency operations in Southwest Asia. This marked the final step in the Air Force's transition from a Cold War, forward-based presence force to one built and shaped for quick and decisive global engagement. Each Air Expeditionary Force (AEF) consists of a small cross-section of aerospace forces, tailored by task, prepared to rapidly deploy and operate from well-established bases or geographically isolated, bare base airfields with minimal infrastructure. These light, lean, and lethal forces rely on advanced communication and information systems as force multipliers and the critical link between the AEF and the Air Force's worldwide support network. This heavy reliance on information connectivity to support sustained operations significantly increases the AEF's vulnerability to information warfare attack.

Terrorists, transnational groups, criminals, and governments all recognize the potential of information warfare (IW). In the United States alone, cyber crime such as intrusion, information theft, data corruption, and system disruption increased 130 percent between 1996 and 1998.[1] The number of intrusions into Department of Defense networks increased from 5,844 in 1998 to over 18,500 in 1999.[2] Major powers including Russia and China continue to develop advanced technologies to mount increasingly effective attacks on information and communication systems. Several of America's potential adversaries already have robust offensive IW capabilities.[3] Because of overwhelming United States (US) military power, most adversaries will likely

[1] Terry Maynard, "Implementing PDD-63: NIPC Progress and Plans" (Speech given at Energy Security Forum, Washington D.C. 19 November 1998).

[2] *Philadelphia Inquirer*, 1 December 1999.

[3] George J. Tenet, "Statement," U.S. Congress, Senate, Select Committee on Intelligence, *The Worldwide Threat in 2000: Global Realities of Our National Security*, Hearings before the Select Committee on Intelligence, 106th Cong, 2nd sess, 2 February 2000.

employ IW as an integral part of an asymmetric engagement strategy. As Senator Jon Kyl, Chairman of the Senate Subcommittee on Technology, Terrorism, and Government Information said, "our enemies needn't risk attacking our strong military if they can much more easily attack our soft digital underbelly."[4] The widespread proliferation of affordable, effective information technology will ensure information warfare's role as a dominant force in future conflicts.

The US military has participated in 50 small-scale contingencies since the end of Operation Desert Storm.[5] United States Air Force forces have played a major role in projecting US power throughout the world. Theater and joint force commanders will rely more and more on the unique abilities of the AEF to meet their needs for aerospace forces. Because mission accomplishment depends so greatly on the uninterrupted flow of accurate and timely information, information warfare poses a significant threat to the AEF.

The following discussion will focus on the information warfare threat to the AEF when deployed to a remote, bare base location with minimal or no supporting infrastructure. This paper will briefly discuss the characteristics of the expeditionary environment, review several key elements of information warfare, examine AEF information connectivity, evaluate critical vulnerabilities of information and communication systems, and identify challenges as well as recommend ways commanders can overcome them when developing strategies to deter, detect, negate, and recover from IW attack.

EXPEDITIONARY ENVIRONMENT

Although originally designed to handle standing contingency commitments, the AEF is prepared to respond to any crisis in any location. Most recent operations involved deploying

[4] *USA Today*, 26 January 1999.

[5] John P. Jumper, "Rapidly Deploying Aerospace Power," *Aerospace Power Journal* (Winter 1999): 4.

United States Air Force (USAF) forces to established bases, unopposed, with in-place supporting infrastructure. Few, if any, deployments have tested the true ability of expeditionary aerospace forces to operate from a bare base location. However, baseline and test deployments to airfields with minimal infrastructure highlight some important characteristics of the expeditionary environment in relation to IW.

Limited Forces

In order to minimize the numbers and size of deployed forces, the AEF relies extensively on "reach-back" to supply capabilities and information not resident within the AEF.[6] Reach-back depends on AEF connectivity over commercial and military information systems. Without connectivity, the AEF loses a significant portion of its combat capability.

Limited Paths of Connectivity

In remote areas, satellite communications (SATCOM) will provide the majority of connectivity outside the AEF. The likelihood of finding sufficient and reliable communication service, especially in undeveloped Third World countries, is doubtful.[7] SATCOM will use both military and commercial satellites for redundancy and to satisfy bandwidth requirements for large data transmissions such as imagery. Cellular phones may supplement SATCOM capabilities, but only for non-secure voice communications.

Within the base, deployed combat communications units will build the communications and information infrastructure from scratch. The time to achieve complete intra-base connectivity will depend on the level of service required and the number of users. In AEF V, the 366th Air Expeditionary Wing transported over 8,000 pounds of cable including 14 miles of

[6] U.S. Joint Chiefs Of Staff, *Information Warfare: A Strategy for Peace...The Decisive Edge in War*, (Washington, D.C.), 3.
[7] Captain Dean Benson, 31 CCS, telephone conversation with author, 13 January 2000.

telephone wire.[8] Technicians took over a week to establish robust service, relying on just a few connections until the network was completed.[9]

Force Protection

Securing and patrolling a defensive perimeter in a completely open, unfamiliar, and possibly hostile environment is difficult. During the no-notice AEF II test deployment, initial manpower shortages caused delays in reinforcing protective barriers against physical attack. An attack conducted against key network components and communications equipment could spell early disaster for the AEF. Coordinating defensive actions without a complete and connected command and control network would prove difficult.

Timing

Time is a critical vulnerability for the AEF. Parts and supplies may take days to arrive rather than hours, depending on shipment priority and airlift availability. This increases the pressure on supply and transportation information systems to get the right piece of equipment to the right place at the right time. It also forces a greater reliance on the automated functions of those systems and reduces the time available for manual intervention. The "Focused Logistics" and "Precision Engagement" elements of Joint Vision 2010 will be put to the test daily. Any significant delay or interruption of resupply will certainly reduce combat effectiveness.

The Air Force has become increasingly dependent on networked information and communication systems to conduct global military operations.[10] Attaining and maintaining connectivity is the biggest IW challenge facing the AEF.

[8] U.S.A.F. Kenney Battlelab, *Wireless Air Expeditionary Force Communications (WAC)*, (Mountain Home A.F.B.: 1999).

[9] Ibid.

[10] Harry D. Raduege Jr., "Defensive Information Operations (DIO) - A J-6 Perspective," *CHIPS*, (Fall 1998).

INFORMATION WARFARE

Much like technology, information warfare is an evolving concept. IW is deeply rooted in the history of conflict under the guise of security and surprise. As early as 500 BC, Sun Tzu wrote, "All warfare is based on deception."[11] Even though definitions and methods of employment have changed and vary among services, the basic foundations of IW remain the same. Joint Publication 3-13 defines IW as "information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries." Air Force Doctrine Document 2-5 retains the joint publication definition but further divides IW into two subsets, offensive counterinformation (OCI) and defensive counterinformation (DCI). This section will focus on the offensive elements of IW and how they relate as a threat to the AEF. The ability to attack information systems revolves around five key elements: psychological operations (PSYOP), electronic warfare (EW), military deception, physical attack, and information attack.

PSYOP is much more complex than dropping leaflets or broadcasting radio messages to entice the enemy to surrender. It involves applications and effects at all levels of war. Strategic PSYOP may take the form of diplomatic announcements or positions. It could also involve releasing selected, modified, or manufactured footage to the media to sway public or international opinion. At a much lower level, it could involve intercepting and rewriting personal e-mail. During Operation Allied Force, servicemembers assigned to Aviano Air Base sent over 42,376 personal e-mails.[12] A carefully scripted and credible plan could exploit feelings of guilt for leaving family members on their own. It might include e-threats from terrorist

[11] Sun Tzu, *The Art of War*, trans. Samuel B. Griffith, (London: Oxford, 1963), 41.
[12] J.F.Smith, "Wired for War: 31st Comm Squadron fights in air campaign," 20 December 1999. <http://www.public.afca.scott.af.mil/public/99dec/dec20.html> (4 January 2000).

groups aimed at relatives and friends. The intense emotional and mental burden, coupled with the additional stress of combat, could easily reduce an individual's warfighting effectiveness to nothing.

EW involves using electromagnetic and directed energy to attack an enemy. The most widely recognized weapons include radar and communication jamming systems and chaff. Because of technological improvements, newer systems are affordable and available on the commercial market. They are highly mobile, employ more sophisticated jamming techniques, and produce greater effects than previous systems. Many older radars like those used for Air Traffic Control are highly vulnerable to jamming. Low power communication and information systems like cellular phones, land mobile radios, and the Global Positioning System can be rendered useless with the proper combination of jamming assets. Future EW may involve electronic attack with conventionally delivered electromagnetic pulse (EMP) weapons. High intensity electromagnetic radiation would permanently destroy the internal circuits of any unprotected electronic device within the effective range of the pulse.

The goal of military deception is to mislead adversaries into acting in accordance with the originator's objectives.[13] During Operation Desert Storm, coalition planners successfully feigned an amphibious landing along the beaches of Kuwait. The deception worked, diverting Iraqi resources and attention away from the real coalition attack. Injecting false returns into a radar system and "leaking" false information are also forms of deception. Deception must be credible to the adversary and thoroughly coordinated to achieve the desired effect.

Physical attack as an element of IW relates to targeting information systems and critical components with firepower. During Operation Allied Force, US forces destroyed several

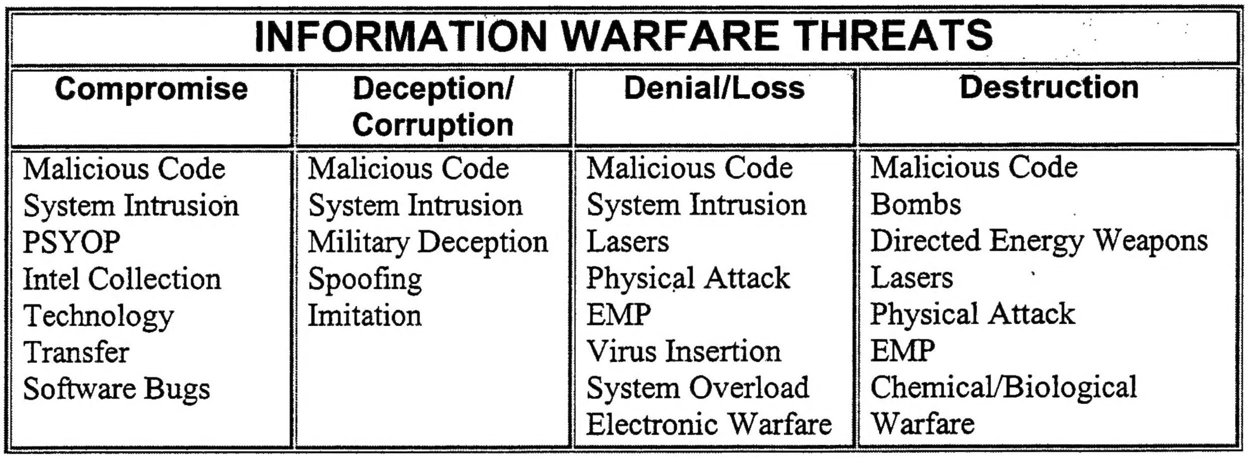
[13] U.S. Air Force, *Information Operations* (Air Force Doctrine Document 2-5) (Washington, D.C.: 5 August 1998), 13.

telephone exchange buildings, severely limiting communications and the flow of information between Serbian military leaders and troops operating in Kosovo.

The final component of offensive IW is information attack. It is essentially the same as physical attack, without the outward appearance of destruction. Computer viruses, malicious code, or manipulating databases destroy or alter an adversary's information or information system without physically destroying the computer or system where it is stored. Availability, simplicity, global connectivity via the Internet, anonymity, and system vulnerability all combine to make information attack the preferred method to wage IW.

IW threats fall into four categories: compromise, deception/corruption, denial/loss, and physical destruction.[14] Figure 1 shows the five offensive IW components grouped according to effect on information and information systems. These components, individually or combined for synergistic effects, pose a significant threat to vulnerable expeditionary aerospace forces.

Figure 1. Information Warfare Threats



INFORMATION WARFARE THREATS			
Compromise	**Deception/ Corruption**	**Denial/Loss**	**Destruction**
Malicious Code System Intrusion PSYOP Intel Collection Technology Transfer Software Bugs	Malicious Code System Intrusion Military Deception Spoofing Imitation	Malicious Code System Intrusion Lasers Physical Attack EMP Virus Insertion System Overload Electronic Warfare	Malicious Code Bombs Directed Energy Weapons Lasers Physical Attack EMP Chemical/Biological Warfare

Source: U.S. Air Force, *Information Operations* (Air Force Doctrine Document 2-5) (Washington, D.C.: 5 August 1998), 6.

[14] U.S. Air Force, *Information Operations* (Air Force Doctrine Document 2-5) (Washington, D.C.: 5 August 1998), 6.

AEF INFORMATION CONNECTIVITY AND VULNERABILITY

The lifeline of the AEF is its connectivity to the outside world. Receiving the Air Tasking Order (ATO), retrieving target imagery and threat information, obtaining meteorological data, ordering supplies and replacement aircraft parts, tracking aircraft and personnel movement, and transmitting mission reports are just a few of the most critical functions any AEF must perform to conduct operations. This discussion will examine each major connectivity component and identify potential vulnerabilities to IW attack.

The Network Control Center (NCC) is the heart of the AEF's information lifeline to the outside world. The NCC monitors, regulates, and protects information flowing through it as well as through connected systems.[15] It contains the routers for the Non-Secure Internet Protocol Router Network (NIPRNET) and the Secure Internet Protocol Router Network (SIPRNET). The phone service trunks and switches are an integral part of the NCC along with the SATCOM link.

Phone transmissions travel through phone lines or a microwave relay and use either the Public Switched Network (PSN) or Defense Switched Network (DSN). They are unencrypted unless the caller is using a STU-III. NIPRNET and SIPRNET transmissions also travel over fixed lines or microwave relays. Information flowing via the NIPRNET to the NCC is usually not encrypted unless the originating program encrypts it. SIPRNET transmissions are always encrypted.

As a transmission travels through the NCC from the phone, NIPRNET, or SIPRNET, it is encrypted before being sent to the satellite. If the phone transmission travels via local telephone trunks, it is not encrypted unless it is a STU-III call. The transmission remains encrypted until it reaches the designated communications support base, where it is deciphered and routed to its

[15] Captain Dean Benson, 31 CCS, telephone conversation with author, 13 January 2000.

final destination. Information traveling to the AEF is encrypted and deciphered in the same way. Even though encryption technology is generally reliable, it cannot protect against all the elements of offensive IW.

The NIPRNET carries the lion's share of sensitive, but unclassified information through cyberspace. Virtually every functional area of the AEF uses the NIPRNET. Critical maintenance systems like the Core Automated Maintenance System track and share data between bases on aircraft status and component failures. The Supply Base Service System also uses the NIPRNET to order spare parts, equipment, and interface with commercial delivery carriers including Federal Express, DHL, and UPS. Using the NIPRNET to enhance mission accomplishment also provides avenues for information attack.

News accounts of computer hacking, destructive viruses, and information theft conducted through the Internet are commonplace. According to Captain Bob West, Deputy Commander of the Joint Task Force on Computer Network Defense, "The NIPRNET is really vulnerable; it has over two million hosts. Information that can be accessed and misused includes troop locations, orders for spare parts, transportation logistics, names of military spouses, and even credit card and telephone numbers."[16] Between 80 and 100 unauthorized intrusions of Department of Defense computers occur each day and during major military operations, the number of intrusions significantly rises.[17]

Launching an information attack on AEF systems through the Internet requires nothing more than a computer and a modem. Even if an adversary could not directly access a military system or network, it is possible to indirectly acquire sensitive data from military related businesses. Penetrating the Federal Express tracking system to determine the type of military

[16] *Philadelphia Inquirer*, 1 December 1999.
[17] Ibid.

cargo shipped as well as the destination might provide the last piece of information necessary to mount a terrorist attack against deployed forces. Obtaining enough unclassified information could provide adversaries with indicators about combat operations, capabilities, vulnerabilities, and intentions.

Information attacks happen at the speed of light. Often, it takes some time to actually determine if an intrusion occurred. Determining the origin of the attack or identifying the attacker is even more difficult, if not impossible.[18] Firewall programs and other security measures may protect systems from most attacks, but not all attacks. The NIPRNET is the single most vulnerable information system used by the AEF.[19]

The SIPRNET is the secure version of the NIPRNET. It uses state of the art encryption technology to safely transport classified information such as intelligence products, imagery, the ATO, and mission reports. This system is highly secure, but for how long? With computer power doubling every 18 months and the continuing technology explosion, an information attack is still a distinct possibility. [20]

If the NIPRNET is the most vulnerable information system used by the AEF, SATCOM is the most vulnerable, and most critical, communications system. During a bare base deployment, SATCOM would provide over 90 percent of communications service off base and use both military and commercial satellites.[21] It is also the primary source of meteorological information from the Defense Meteorological Satellite System. Operation Allied Force used an incredible amount of satellite capacity despite being conducted from well established bases

[18] Ibid.

[19] Interview, Captain Dean Benson, 31 CCS, 11 January 2000.

[20] Ibid.

[21] Ibid.

throughout Europe. Key satellite vulnerabilities include signal interception and access denial by jamming or destroying uplink and control equipment.

The AEF may also use cellular phones to reduce the amount of time required to set up communications infrastructure. Most digital cellular service providers claim their systems offer a high degree of protection against compromise and deception. Are they lying? In 1998, researchers in San Francisco successfully cracked the digital algorithm for the Groupe Speciale Mobile (GSM) standard.[22] It took a computer over 10 hours to break the code, but proves with determination and the right technology anything is possible. GSM is the most widely available service in Europe. An AEF deployment to a remote part of Europe might have to rely on cellular communications using the GSM standard.

Cellular phones can easily be located within 125 meters of their actual position.[23] For a fee, some cellular companies can provide enhanced services to accurately position the phone within 30 meters of its actual location.[24] A terrorist armed with the phone numbers of key AEF personnel could easily monitor and predict the movements of potential high value targets. Additionally, cellular phones are susceptible to denial and loss of signal. They typically operate at low power levels allowing a jammer to cover any signal with very little effort.

The Land Mobile Radio (LMR) also provides portable, lightweight, handheld communications. The LMR is also capable of secure transmissions…but how secure? The encryption algorithm is commercially produced by Motorola and can be deciphered. Additionally, LMRs also produce low power and can be jammed much like cellular phones. The LMR network is vulnerable to compromise, deception, denial, and destruction.

[22] John Markoff, "Researchers Crack Code in Cell Phones," 28 April 1998. <http://www.info-sec.com/abuse/abuse_042898a_j.html-ssi> (26 January 2000).
[23] *Mobile Positioning: An Introduction to Mobile Positioning.* 1 December 1999. <http://www.mobilePositioning.com> (27 December 1999).

Except for the PSN, the local base infrastructure is not in itself an information system but is vulnerable to physical attack, deception or corruption of key automated functions, and denial of control. Even though the AEF commander is not directly responsible for protecting infrastructure elements beyond the base fence, it is important to work with the host nation to provide support and offer guidance on how to protect a vital resource against an IW attack.

Deployed AEF forces, linked to the outside world through several critical but vulnerable systems, must take steps to protect those systems from attack. The IW threat is significant to deployed aerospace forces. Analyzing the potential effects of an adversary's information attack can help identify the best course of action to deter, detect, negate, and recover from IW attacks.

CHALLENGES AND RECOMMENDATIONS

Host Nation Infrastructure

Basic utilities such as water, electricity, and phone service may be supplied by the host nation. Just how secure are they against the IW threat? Public services in many countries are not as advanced as those in the US and correspondingly less susceptible to cyber or electronic attack. However, they are still vulnerable to physical attack. In some instances, the AEF may be forced to rely on local infrastructure for a substantial portion of the support necessary to sustain operations. Theater commanders should incorporate infrastructure support assessment for the most likely deployment areas into standing plans. Assigning the responsibility to compile and disseminate this information to the Contingency Response Group, discussed later, will help ensure the AEF brings the right equipment to accomplish the mission. A reliable and secure infrastructure minimizes the need for excess equipment, saving support sorties for more critical missions. Conversely, deploying with adequate equipment to supplement or replace the

[24] Ibid.

airfield's infrastructure would keep the AEF in operation if service were interrupted. Implementing a plan to assess the threat and help the host nation defend the infrastructure supporting the airfield against an IW attack is critical to mission success.

Physical Security

Establishing and maintaining a secure environment large enough to negate the effect of mobile electronic jammers or to deter a physical attack on the base may be difficult. Electronic jamming and eavesdropping devices can operate effectively from long distances. Modern explosive weapons need only detonate close to the target to cause significant damage. Host nation sensitivities, political concerns, and available resources may dictate a compromise in optimum security measures. Few countries will grant the US an unrestricted license to use force against their citizens or property. Coordinating defensive measures with the host nation also presents problems. US efforts to take action might be viewed as too aggressive. Releasing highly classified information about a specific threat may cost more in terms of revealing US intelligence capabilities than the potential impact of the threat on AEF operations. Negotiating host nation support agreements that allow appropriate measures against IW as well as physical attack would improve the AEF's overall defensive posture.

Controlling Information Access

Attacks on information systems can originate from outside or inside the system. Adaptive protection software, firewalls, and authentication procedures can shield the system from outside intrusion. However, an attack from behind this safety shield has the potential for widespread damage, whether intentional or inadvertent. The unauthorized use of a mission essential computer to retrieve personal e-mail could allow an outsider instant access to the most critical areas of an information system.

The availability and low cost of information technology puts cellular phones and other personal communication devices in the hands of just about anyone, including deployed troops. An unsuspecting airman might give away sensitive, unclassified information by just using these devices. Mobile positioning systems can accurately locate a cellular phone user within 30 meters.[25] Discussing a work schedule or simply maintaining a consistent pattern of calls might give adversaries clues about operational timing. Phones with access to the Internet might provide uncontrolled conduits for PSYOP through intercepted and altered e-mails or e-threats against friends and family.

Programs such as the Multilevel Information Systems Security Initiative (MISSI) offer the AEF writer-to-reader information security services such as data integrity, access control, authentication, non-repudiation, and confidentiality.[26] This system uses small electronic cards, issued to all authorized users, to grant access to the network, encrypt all outgoing transmissions, and decipher incoming messages. It protects sensitive unclassified information as it travels over the Internet. This program is in the early stages of implementation. Shifting the priority to equip deploying AEF units first would help reduce network vulnerability to information attack. Establishing criteria, methods, and policy to control and safeguard the use of personal and official communications devices is another important requirement to protect forces from IW.

Training and Doctrine

Although the Air Force changed its doctrine to reflect the latest concepts and definitions of IW, pre-deployment training still remains focused on operations security. Airmen and officers outside information operations career fields receive little training on any other element of IW.

[25] *Mobile Positioning: An Introduction to Mobile Positioning.* 1 December 1999. <http://www.mobilePositioning.com> (27 December 1999).
[26]. Bill James, "Air Force applies strategy to protect information," 26 July 1998. <http://www.af.mil/news/Jul1996/n19960724_960713.html> (10 January 2000).

As an example, physical attack is covered in the force protection briefing given just prior to deployment, but only as it relates to potential terrorist attacks on military personnel. Since IW permeates all aspects of military action, pre-deployment training should include increased emphasis on all the elements of IW, especially defensive measures such as recognizing and reporting a suspected IW attack.

Contingency Response Group (CRG)

The United States Air Forces in Europe created a new organization to expedite the deployment and employment of the AEF. As an advance element of the AEF, the CRG provides the first on-scene Air Force forces trained to command, assess, and prepare a base for expeditionary aerospace forces.[27] The group consists of 134 personnel representing more than 40 diverse specialties. The number of assigned personnel can expand to include as many as 2,000 to handle large-scale deployments of more than one AEF. During Joint Task Force Shining Hope, the CRG transformed a bare base airfield at Tirana into a major aerial port, boosting its handling capacity from 10 takeoffs and landings a day to over 400. The group does include a PSYOPS representative, but only as an augmentee for larger deployments. Creating a permanent billet for an IW expert in the basic group would ensure the full integration of defensive and offensive IW from the very beginning of any operation. Also, establishing a CRG structure within each major command would allow the members of the group to concentrate their preparations on just one theater and better support AEF deployments.

CONCLUSION

Information warfare is a significant threat to the AEF. As the Air Force seeks new ways to further reduce the AEF's logistical and force footprints, information and communication systems will play an even more crucial role in mission accomplishment. This in turn will lead to greater exposure and vulnerability to IW attack, especially as combatant commanders increasingly rely on the AEF for deployed aerospace power. Commanders at all levels need to understand the nature of the IW threat to AEF forces to better coordinate actions to deter, detect, negate, and recover from IW attack.

The greatest IW threats to the AEF include physical attack, information attack, electronic warfare, and psychological operations. The focus of these threats is to deny the use of critical information systems, delay and distort the entire flow of information supporting operations, and ultimately eliminate the AEF as an effective fighting force. Working with the host nation to protect deployed forces and the local infrastructure, carefully controlling access to critical information systems, improving the depth and focus of IW training, and increasing the number of deployed IW experts will help shield AEF vulnerabilities from the threat. Protecting the critical information systems that support and sustain AEF operations is a shared responsibility among theater, operational, and tactical commanders. Although no system is completely secure, incorporating these changes will ensure the AEF remains a strong and integral component of US military power.

[27] John P. Jumper, "Rapidly Deploying Aerospace Power," *Aerospace Power Journal*, Winter 1999, 5.

BIBLIOGRAPHY

Benson, Dean, Captain, USAF, 31 CCS. Telephone conversation with author, 13 January 2000, Newport, R.I.

Buchanan, Glenn C. "Implications of Information Vulnerabilities for Military Operations." In *The Changing Role of Information in Warfare,* ed. Zalmay M. Khalilzad and John P. White, 283-323. Santa Monica: Rand, 1999.

Denning, Dorothy E. *Information Warfare and Security.* Reading: Addison Wesley, 1999.

James, Bill. "Air Force applies strategy to protect information". July 1996. <http://www.af.mil/news/Jul1996/n19960724_960713.html> (10 January 2000).

Jumper, John P. "Rapidly Deploying Aerospace Power." *Aerospace Power Journal*, Winter 1999, 4-10.

Kenyon, Henry S. "Adaptive Response Tool Foils Hacker Intrusion." August 1999. <http://www.us.net/signal/Archive/August99/adaptive-aug.html> (9 January 2000).

Libicki, Martin C. "Information Dominance." *Strategic Forum*, Number 132, November 1997. <http://www.ndu.edu/inss/strforum/forum132.html> (29 November 1999).

Looney, William R. "The Air Expeditionary Force: Taking the Air Force into the Twenty-first Century." *Airpower Journal*, Winter 1996.

Markoff, John. "Researchers Crack Code in Cell Phones," 28 April 1998. <http://www.info-sec.com/abuse/abuse_042898a_j.html-ssi> (26 January 2000).

Maynard, Terry. "Implementing PDD-63: NIPC Progress and Plans." Speech given at Energy Security Forum, Washington D.C., 19 November 1998.

Mobile Lifestreams. *Mobile Positioning: An Introduction to Mobile Positioning.* 1 December 1999 <http://www.mobilePositioning.com> (27 December 1999).

Raduege, Harry D. Jr. "Defensive Information Operations (DIO) - A J-6 Perspective." *CHIPS*, Fall 1998.

Robinson, Clarence A. Jr., "China's Military Potency Relies On Arms Information Content." November 1999. <http://www.us.net/signal/Archive/Nov99/china-nov.html> (9 January 2000).

Tzu, Sun. *The Art of War.* Translated by Samuel B. Griffith. London: Oxford, 1963.

U.S. Air Force. Information Operations (Air Force Doctrine Document 2-5) Washington, D.C.: 5 August 1998.

U.S. Air Force Kenney Battlelab. *Wireless Air Expeditionary Force Communications (WAC).* Mountain Home A.F.B.: 1999.

U.S. Congress. Senate. Select Committee on Intelligence. *The Worldwide Threat in 2000: Global Realities of Our National Security.* Hearings before the Select Committee on Intelligence. 106th Cong, 2nd sess, 2 February 2000.

U.S. Joint Chiefs of Staff. *Information Warfare: A Strategy for Peace...The Decisive Edge in War.* Washington, D.C.

U.S. Joint Chiefs of Staff. *Joint Doctrine for Information Operations* (Joint Pub 3-13) Washington, D.C.: 9 October 1998.